

11/09/99 Jc690 U.S. PTO

Jc511 U.S. PTO  
09/437065  
11/09/99 A

In the United States Patent and Trademark Office

In re Application of:

Assignee: Arcot Systems, Inc.  
Inventors: Balas Natarajan Kausik, Ph.D.  
Serial No: Unknown  
Filed: Herewith  
For: Method and System For Secure Authen-  
ticated Payment On A Computer Network

CERTIFICATE OF MAILING  
BY "EXPRESS MAIL" UNDER 37 CFR § 1.10

"Express Mail" Mailing Label Number  
EL441851887US

Date of Deposit: November 9, 1999

I hereby certify that this paper and all enclosures  
are being deposited with the United States Postal Service  
"Express Mail Post Office to Addressee" under 37 CFR §  
1.10 on the date indicated above and is addressed to the  
Assistant Commissioner for Patents, Washington, D.C.  
20231

Type or Print Name of Person Mailing: Paulette D. Isler  
Signature of Person Mailing: *Paulette D. Isler*

PATENT APPLICATION TRANSMITTAL LETTER

Assistant Commissioner for Patents  
BOX PATENT APPLICATION  
Washington, D.C. 20231

Sir:

Transmitted herewith for filing in connection with the above-identified patent  
application are the following:

<u>X</u>	<u>5</u>	Sheets of drawings	<u>X</u>	Formal
				Informal
		Assignment and Assignment Recordation Cover Sheet.		
		Verified Statement Claiming Small		Signed
		Entity Status		Unsigned
		Information Disclosure Statement		
		Certified Copy of Priority Document		
<u>X</u>		Declaration for Patent Application	<u>X</u>	Signed
				Unsigned
<u>X</u>		Unexecuted Power of Attorney by Assignee of Patent Application		
		Before calculating the fee, cancel		

[illegible]

SMALL ENTITY	
Rate	Fee
	\$ 380.00
x 9.00	\$ 0
x 39.00	\$ 0
+130	\$
TOTAL:	\$

X A check in the amount of \$ 760.00 (Check No. 2237) to cover the filing fee is enclosed.

\_\_\_\_\_ Fee for Assignment Recordation (separate check enclosed) \$40.00  
(Check No. \_\_\_\_\_).

X The Commissioner is hereby authorized to charge any additional fees which may be required in this application under 37 C.F.R. Sections 1.16-1.17 during its entire pendency, or credit any overpayment, to Deposit Account No. 19-2385. Should no proper payment be enclosed herewith, as by a check being in the wrong account, unsigned, post-dated, otherwise improper or informal, or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-2385. This sheet is filed in duplicate.

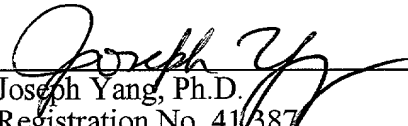
Address all future communications to:

Joseph Yang, Ph.D.  
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP  
525 University Avenue  
Palo Alto, California 94301  
(650) 470-4500

Date: Nov. 9, 1999

Respectfully submitted,

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

By:   
\_\_\_\_\_  
Joseph Yang, Ph.D.  
Registration No. 41,387

**METHOD AND SYSTEM FOR SECURE AUTHENTICATED  
PAYMENT ON A COMPUTER NETWORK**

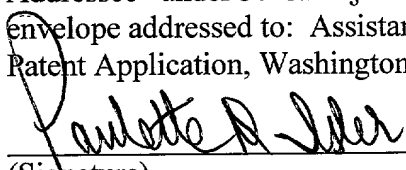
**Inventors:**

Balas Natarajan Kausik, Ph.D.

**Prepared By:**

Joseph Yang, Ph.D.  
Skadden, Arps, Slate, Meagher & Flom LLP  
525 University Avenue  
Palo Alto, California 94111  
(650) 470-4500

I hereby certify that this correspondence is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" under 37 CFR § 1.10 (Label No. EL441851887US) in an envelope addressed to: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231, on 11-9-99.

  
(Signature)

11/9/99  
(Date)

# **METHOD AND SYSTEM FOR SECURE AUTHENTICATED PAYMENT ON A COMPUTER NETWORK**

## **FIELD OF THE INVENTION**

5

The present invention relates to a method and system for secure authenticated payment at a point-of-sale on a computer network. More particularly, the present invention allows the use of digital signatures on a sales draft to authenticate purchasers in a manner that does not necessarily require any changes in the transaction processing of the financial institutions participating in the transaction.

10

## **BACKGROUND OF THE INVENTION**

In present electronic commerce transactions, buyers may pay for goods and services by presenting the seller with a payment card number, e.g., a conventional credit card number. Because the buyer and seller are connected solely through a computer network (e.g., the Internet), it is not possible for the buyer to authenticate himself as the legitimate cardholder, nor can the buyer sign the sales draft. Thus, the seller honors any valid credit card number that is presented, creating a large opportunity for fraud.

15

Worse yet, other forms of payment such as debit cards are not presently viable on computer networks. Debit cards require the cardholder to enter a personal identification number ("PIN"), which is used to authenticate the transaction to the cardholder's bank. However, entering a simple PIN on a networked computer poses a substantial security risk—if the PIN and the debit-card number fell into the wrong hands, the cardholder's bank account would be completely compromised.

20

25

Thus, with respect to both conventional credit and debit cards, authenticating a cardholder on the network with a solution that is simple, secure, and easy to deploy remains an important unsolved problem.

30

Digital signature technology offers one means of authenticating the cardholder with a high degree of security. In this technology, each cardholder owns a pair of keys –

a signature (private) key and a verification (public) key. The cardholder signs a transaction with his private key, and then sends the transaction, the digital signature, and (optionally) his public key to the merchant. The merchant forwards these items to the bank (or other financial institution), and the bank honors the transaction if the  
5 cardholder's public key verifies the cardholder's digital signature.

One security advantage of digital signatures is that the private key of the cardholder typically remains in possession (or at least control) of the cardholder. Thus, there is no inherent risk associated with a transaction that would compromise future transactions. One disadvantage of the digital signature method described above is that  
10 banks and transaction processors would have to change their existing infrastructure to allow digital signatures to flow through their networks. This infrastructure change would basically require a substantial overhaul of the present electronic banking and transaction processing system, which is costly and difficult to achieve.

Thus, there is a need for a method and system that offers the security advantages  
15 of digital signatures without necessarily requiring significant changes in the banking and processing network.

## SUMMARY OF THE INVENTION

20 One embodiment of the present invention includes a simple, secure and easy-to-deploy method and system for authenticating credit and/or debit cardholders at a point-of-sale on a computer network (e.g., the Internet). Cardholders are authenticated using digital signatures on a sales draft, in a manner that does not necessarily require any changes in the transaction process of the financial institutions participating in the  
25 transaction.

In this embodiment of the system, the cardholder enrolls for an electronic payment card (either an electronic debit or credit card) at a participating financial institution by visiting its issuer proxy enrollment site, e.g., a web site hosted by an issuer proxy computer associated with the financial institution. At the enrollment site, the  
30 cardholder types in his particulars, such as his conventional payment card number,

conventional payment card PIN, name, address, etc. The cardholder also (optionally) selects a password (access code) for his electronic payment card that is preferably unrelated to the PIN for his conventional payment card. The issuer proxy generates a public key-private key pair for use by the cardholder if the cardholder does not already have such a pair. The issuer proxy binds the cardholder's public key and some or all of the cardholder's payment particulars in a digital certificate using an encryption key (called a domain key) that is shared between the issuer proxy and a bridge computer. Such a domain key will allow the bridge computer to confirm the issuer's certification during a subsequent authorization stage, described below. The cardholder then receives a piece of software that is downloaded to his computer containing his particulars in encrypted form. This piece of software constitutes the cardholder's electronic payment card. It comprises (or is configured to obtain and use) the cardholder's private key, which is (optionally) protected by the password, and the corresponding public-key digital certificate containing the cardholder's payment particulars.

Thenceforth, as the cardholder shops online, he can elect to pay via electronic payment. To do so, the cardholder activates his electronic payment card with the previously selected password. The cardholder's electronic payment card software interacts with corresponding software at the online merchant to digitally sign the sales draft created during the transaction with the cardholder's private key. The merchant then sends the signed sales draft and the cardholder's digital certificate to the bridge computer for processing. The bridge computer uses the cardholder's digital certificate to check the digital signature on the sales draft. If the signature is valid, the bridge computer creates a conventional debit or credit transaction to be processed by the banking and transaction network. The particulars needed for creating the conventional transaction, such as the conventional card number and PIN, are extracted and decrypted from the cardholder's digital certificate using the private key associated with the domain key (if the digital certificate was asymmetrically encrypted) or the domain key itself (if the digital certificate was symmetrically encrypted). The embodiment of the invention described above provides one or more of the following advantages:

- (1) Additional hardware at the cardholder's computer is not necessarily required for deployment. This is in marked contrast to hardware tokens such as smart cards, where cards and card readers are required. Of course, the software comprising the cardholder's electronic payment card can be stored on smart cards, as well as virtually any other storage medium, including, without limitation, floppy disks, hard drives, and magnetic stripe cards;
- (2) Changes are not necessarily required in the existing banking network;
- (3) Administrative overhead is low. The cardholder can enroll at any participating financial institution that offers the service, not necessarily the one that issued the cardholder's conventional payment card. Furthermore, enrollment can be on a self-serve basis and does not necessarily require activation mailings by the financial institutions;
- (4) Electronic payment cards can be deployed rapidly, because they are intuitive to use and require little user or administrator training; and/or
- (5) Security can be enhanced via special techniques such as "cryptographic camouflaging," which is commercially available from Arcot Systems, Inc.

The foregoing and other embodiments and aspects of the present invention will become apparent to those skilled in the art in view of the subsequent detailed description of the invention taken together with the accompanying figures and appended claims.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating an exemplary computer system for secure authenticated payment on a computer network.

FIG. 2 is a flow chart illustrating an exemplary method for cardholder enrollment for an electronic payment card.

FIG. 2A illustrates an exemplary electronic payment card created using the preferred embodiment of the invention.

FIG. 3 is a flow chart illustrating an exemplary method for point-of-sale interaction between a cardholder and a merchant.



FIG. 4 is a flow chart illustrating an exemplary method for a merchant to obtain authorization for the payment transaction.

## DETAILED DESCRIPTION OF THE INVENTION

5

FIG. 1 is a block diagram illustrating an exemplary computer system for secure authenticated payment on a computer network (e.g., the Internet). The system contemplates a network of computers including a cardholder's computer **100**, a payment card issuer's proxy computer **110**, a merchant's computer **120**, a bridge computer **130**, a payment gateway computer **140**, and legacy backend computer **150**. In this exemplary embodiment, the network is deployed over the Internet, although those skilled in the art will recognize that any public or private communication network including, without limitation, extranets, intranets, and other telephonic or radio communications networks could also be used. Similarly, as used herein, the term computer refers to any device that processes information using an integrated circuit chip, including without limitation mainframe computers, work stations, servers, desktop computers, portable computers, embedded computers, and hand-held computers.

### Enrollment

Referring now to FIG. 2, at step **200**, a cardholder (user) at computer **100** enrolls for an electronic payment card (either an electronic debit card or an electronic credit card) at the electronic payment card issuer proxy **110**, typically by visiting the website of a participating financial institution on the Internet. At step **210**, the cardholder provides the issuer **110** with particular information used to make a payment (payment particulars), such as his conventional payment card number, conventional payment card PIN, conventional credit card holder verification value 2 ("CVV2"), conventional cardholder name and address, or any other cardholder identification information. The issuer proxy **110** can be operated by any trusted financial institution that participates in the electronic payment system, not necessarily the financial institution that issued the cardholder's conventional payment card.

The issuer proxy **110** can optionally verify the cardholder's payment information by any of the means available for such verification including, without limitation, creating a payment transaction in the conventional payment network. Such a transaction could be "authorization only" in the sense that it would be used only for verifying the cardholder's payment particulars, with no money actually transferred.

At step **220**, the issuer **110** generates a public key-private key pair for the cardholder to use in connection with the electronic payment system. If the cardholder already has a public key-private key pair that he wishes to use in connection with the electronic payment system, he provides his public key to the issuer **110**. The cardholder's private key is typically stored on the cardholder's computer **100**, often under the control of a PIN or other form of access code (password). The access code can be protected against unauthorized detection using commercially available software technology such as software smart cards from Arcot Systems, Inc., described in "Software Smart Cards via Cryptographic Camouflage," Proceedings IEEE Symposium on Security and Privacy, May 1999, and in co-pending US patent application number 08/996,758, "Method and Apparatus for Secure Cryptographic Key Storage Certification and Use," which is incorporated herein by reference.

The access code may also be protected against unauthorized detection (e.g., so-called "shoulder surfing") using the technology described in co-pending US patent application number 09/249,043, "Method and Apparatus for Secure Entry of Access Codes in a Computer Environment," which is incorporated herein by reference.

At step **230**, the issuer **110** binds the cardholder's public key and some or all of the cardholder's payment particulars in a digital certificate, typically by encrypting the cardholder's public key and particular identifying information provided by the cardholder. The encryption key used for encrypting the cardholder's payment particulars – called the domain key – is typically shared between the issuer proxy **110** and the bridge computer **130**, and may be either a symmetric key or an asymmetric encryption key. In one embodiment, the domain key may be a public key associated with the bridge computer **130**, so that only the bridge computer **130** can decrypt the encrypted cardholder particulars (using a corresponding private key associated with the bridge computer **130**). In another embodiment, the domain key may be a symmetric encryption key that is

shared by the issuer proxy **110** and the bridge computer **130**. In either case, the bridge computer will use the domain key (actually, its private key counterpart, if asymmetric; or the domain key itself, if symmetric) to verify the binding, as will be described later in the section entitled "Authorization." After the issuer proxy **110** combines the cardholder's public key with some or all of the cardholder's payment information and digitally signs the combination to create a digital certificate for the cardholder, the digital certificate for the cardholder is loaded into an electronic payment card for the cardholder. Of course, those skilled in the art will realize that many other types of binding can be used including, without limitation, offloading the signing to a trusted third party, or receiving (rather than creating) the digital certificate from the user (although such binding is less secure).

At step **240**, the issuer **110** sends and the cardholder's computer **100** receives the cardholder's electronic payment card, e.g., a piece of software that is downloaded to the cardholder's computer **100**. The electronic payment card (typically stored in a software wallet) may be further protected against unauthorized access via a PIN (preferably different from the PIN associated with the cardholder's conventional payment card) or other form of user access code. The access code may be protected against unauthorized detection by the above-mentioned procedures used to protect the private key PIN. (Indeed, if the two PINs are the same, private key access for digitally signing and electronic payment card access for transaction execution could be accessed via a single protocol.) Setting the access code (PIN) for the electronic payment card is preferably done when the electronic payment card is being created by the issuer **110**, but can also be done separately, e.g., when the cardholder first accesses his electronic payment card on the cardholder computer **100**.

Alternatively, if the cardholder wishes to be able to perform electronic transactions from a variety of locations, the cardholder's private key and/or electronic payment card may be stored at a credential server and downloaded on the fly by a roaming cardholder using a shared secret or challenge-response protocol. In the latter case, commercially available software such as Arcot WebFort from Arcot Systems, Inc., described at <http://www.arcot.com/products.html> and in co-pending U.S. patent application number 09/196,430, "Method and Apparatus for Secure Distribution of

Authentication Credentials to Roaming Users,” which is hereby incorporated by reference, may be used to effect the roaming functionality.

One advantage of this enrollment process is that the issuer’s participation can be passive, in that the issuer proxy **110** can be operated by any trusted financial institution that participates in the electronic payment system, and is not necessarily the bank or financial institution that issued the conventional payment card to the cardholder. This is important because it suffices that one well-recognized financial institution participates in the system. Furthermore, even the participation of this financial institution can be limited to establishing the issuer proxy **110** on the network for self-service access by the cardholder, and does not require mailings to the cardholder, or other physical interaction with the cardholder.

FIG. 2A illustrates an exemplary electronic payment card created using the preferred embodiment of the invention, in which the card contains: (a) the cardholder’s digital certificate, comprising the cardholder’s payment particulars, and his public key, portions of which are encrypted under the domain key; and (b) the cardholder’s private key.

#### Point-of-sale Transaction between a Cardholder and a Merchant on the Computer Network

A cardholder uses his computer **100** to shop at a merchant’s website at merchant’s computer **120**. Referring now to FIG. 3, at step **300**, when the cardholder decides what goods or services he wants to buy, the merchant presents the cardholder with an electronic sales draft.

At step **310**, the cardholder elects to pay the sales draft using the cardholder’s electronic payment card. At step **320**, a representation of the cardholder’s electronic payment card may be displayed on the cardholder’s computer **100**. If the cardholder chose to protect his electronic payment card with an access code, then at step **330** the cardholder unlocks and activates his electronic payment card. If the electronic payment card is protected with an access code, then the electronic payment card cannot be activated unless the correct access code is entered. The access code can be stored in a variety of locations including, without limitation, the cardholder’s own memory, or a

floppy disk, magnetic stripe card, smart card, or disk drive coupled to the cardholder's computer **100**. At step **340**, the cardholder's (activated) electronic payment card digitally signs the electronic sales draft that was presented to the cardholder in step **300** using the cardholder's private key. Optionally, the cardholder's electronic payment card can  
5 automatically fill in the information used by the sales draft. At step **350**, the cardholder's computer **100** sends the digitally signed sales draft and the cardholder's digital certificate to the merchant's computer **120**, where it is received by the merchant's computer **120**.

#### Authorization

10 Referring now to FIG. 4, at step **400**, the merchant's computer **120** sends, and the bridge computer **130** receives, an authorization request from the merchant (seller). The authorization request includes the electronic sales draft with the cardholder's (buyer's) electronic signature and the cardholder's digital certificate. As mentioned above, in one embodiment of the invention, the cardholder's digital certificate includes the cardholder's  
15 verification key (public key) and an encrypted version of the cardholder's PIN for his conventional payment card.

At step **410**, the bridge computer **130** uses the cardholder's verification key to confirm (verify) that the cardholder's electronic signature on the sales draft was authorized by the cardholder (buyer). If the electronic signature is confirmed, then at step  
20 **420** the bridge computer **130** extracts the encrypted version of the cardholder's PIN for his conventional payment card from the cardholder's digital certificate and decrypts the PIN using the private key associated with the domain key (if the PIN was asymmetrically encrypted) or the domain key itself (if the PIN was symmetrically encrypted). In this (or in some equivalent) fashion, the bridge computer **130** can verify the binding (of the  
25 payment particulars and the user's public key) that was performed by the issuer **110**. The bridge computer **130** uses the decrypted PIN to generate a conventional authorization request as is well-known to those skilled in the art of payment card transaction processing (see, e.g., Visa International Acquirer Services External Interface Specification, April 1 1999, EIS 1080 Version 5.8, available from Visa). The decrypted PIN may be re-  
30 encrypted with a key that is shared by the bridge computer **130** and the transaction processor at payment gateway **140**. Certain other particulars that are typically used for

creating a conventional authorization request, such as the conventional payment card number, conventional credit card holder verification value 2 (“CVV2”), conventional cardholder name and address, or any other cardholder identification information, may also be extracted and decrypted from the cardholder’s digital certificate.

5           Note that some types of conventional payment transactions do not necessarily use PINs, e.g., some conventional credit card transactions. For these transactions, after the bridge computer **130** verifies the cardholder's digital signature on the sales draft at step **410**, the bridge computer **130** generates a conventional authorization request at step **420** without performing the PIN extraction and PIN decryption steps.

10           At step **430**, the bridge computer **130** sends the conventional authorization request to the transaction processor at payment gateway **140**. Using the information provided in the authorization request, the payment gateway **140** approves or denies the request and sends its authorization response back to the bridge computer **130**.

15           In an alternative embodiment of the invention, the bridge computer **130** can be integrated into the payment gateway **140**. Indeed, any combination of issuer proxy **110**, bridge computer **130**, and/or payment gateway **140** can be integrated together.

20           The bridge computer **130** receives from the payment gateway **140** either an approval or a disapproval of the authorization request. In either event, at step **440**, the bridge computer **130** forwards the authorization response (approval or disapproval) to the merchant (seller) at the merchant’s computer **120**.

          If the cardholder is making a debit transaction, then at step **450** the merchant’s computer **120** sends a confirmation to the payment gateway **140** via the bridge computer **130**.

25           One advantage of this authorization process is that there is minimal impact on the merchant. Another advantage is that the payment gateway **140** can interact with the legacy back-end systems **150** using conventional transaction processing methods. In other words, no changes are necessarily required to the back-end infrastructure.

30           In an alternate embodiment of the system, the bridge computer **130** can act in “stand-in” mode. Specifically, some financial institutions may choose not to receive the decrypted PIN from the cardholder’s digital certificate, relying instead on the bridge computer’s assertion that the cardholder’s signature verified correctly. If the cardholder

PIN was also verified at the issuer proxy 110 during enrollment, the risk of a fraudulent transaction may be deemed low. In such situations, the bridge computer 130 would assemble and transmit an authorization request without a PIN to the transaction processor at payment gateway 140.

5 In yet another embodiment of the system, the merchant can store a copy of the digital signature of the cardholder along with the sales draft. The bridge computer 130 would process the transaction assuming that the digital signature of the cardholder is valid. In the event that the cardholder disputes the transaction, the merchant must present the stored copy of the sales draft and the cardholder's digital signature. The bridge  
10 computer 130 will verify the digital signature and, on the basis of the verification, determine whether the merchant should refund the amount of the transaction. An advantage of this embodiment is that the computational processing required at the bridge computer 130 is reduced. However, the merchant faces an increased risk of fraud.

In yet another embodiment of the system, a user who does not have a  
15 conventional credit or debit card (or who wants to get additional conventional payment cards), can be given the option of signing up for a conventional payment card during the electronic payment card enrollment process. The conventional payment card number that is given to this user can then be incorporated into the user's electronic payment card.

In yet another embodiment of the system, a user may choose to enroll his  
20 checking account to an electronic payment credential, rather than a debit or credit card. The user would identify himself via a variety of means at enrollment time, or may be given an activation code by his bank that he would use to identify himself for enrollment.

Although the preferred embodiments of this invention create an electronic  
25 payment card for conventional debit or credit cards or conventional checking accounts, the present invention enables a bridge to network payment for almost any conventional transaction system. For example, the present invention could also be used for secure electronic bill payment, person-to-person transactions, and electronic auction settlements.

The software described herein, for use by the various computers, is conveniently  
30 implemented using C, C++, Java, Javascript, HTML, or XML, running on Windows, Windows NT, Solaris, Unix, Linux, or Macintosh operating systems on virtually any

computer platform. Moreover, those skilled in the art will readily appreciate that such software can be implemented using virtually any programming language, running on virtually any operating system on any computer platform.

The various embodiments described above should be considered as merely illustrative of the present invention. They are not intended to be exhaustive or to limit the invention to the forms disclosed. Those skilled in the art will readily appreciate that still other variations and modifications may be practiced without departing from the general spirit of the invention set forth herein. Therefore, it is intended that the present invention be defined by the claims that follow.

10

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000



What is claimed is:

1. A method for authenticating an electronic payment comprising:

- 5 receiving from a seller an electronic sales draft including an electronic signature;
- receiving from said seller a digital certificate associated with a buyer, said digital certificate including a verification key and an encrypted version of a personal identification number (PIN);
- 10 using said verification key to verify that said electronic signature was authorized by said buyer;
- extracting said encrypted version of said PIN from said digital certificate;
- decrypting said encrypted version of said PIN;
- generating, using said PIN, an authorization request;
- sending said authorization request for a PIN to a financial institution;
- 15 receiving an approval of said authorization request from said financial institution; and
- sending said approval to said seller.

## ABSTRACT

A simple, secure and easy-to-deploy method and system for authenticating credit and debit cardholders at the point-of-sale on a computer network (e.g. the Internet) is disclosed.

Cardholders are authenticated using digital signatures on a sales draft, in a manner that does not

5 necessarily require any changes in the transaction flow of the participating financial institutions.

11/11/2011 11:11:11 AM

FIG. 1 is a block diagram of a payment system architecture.

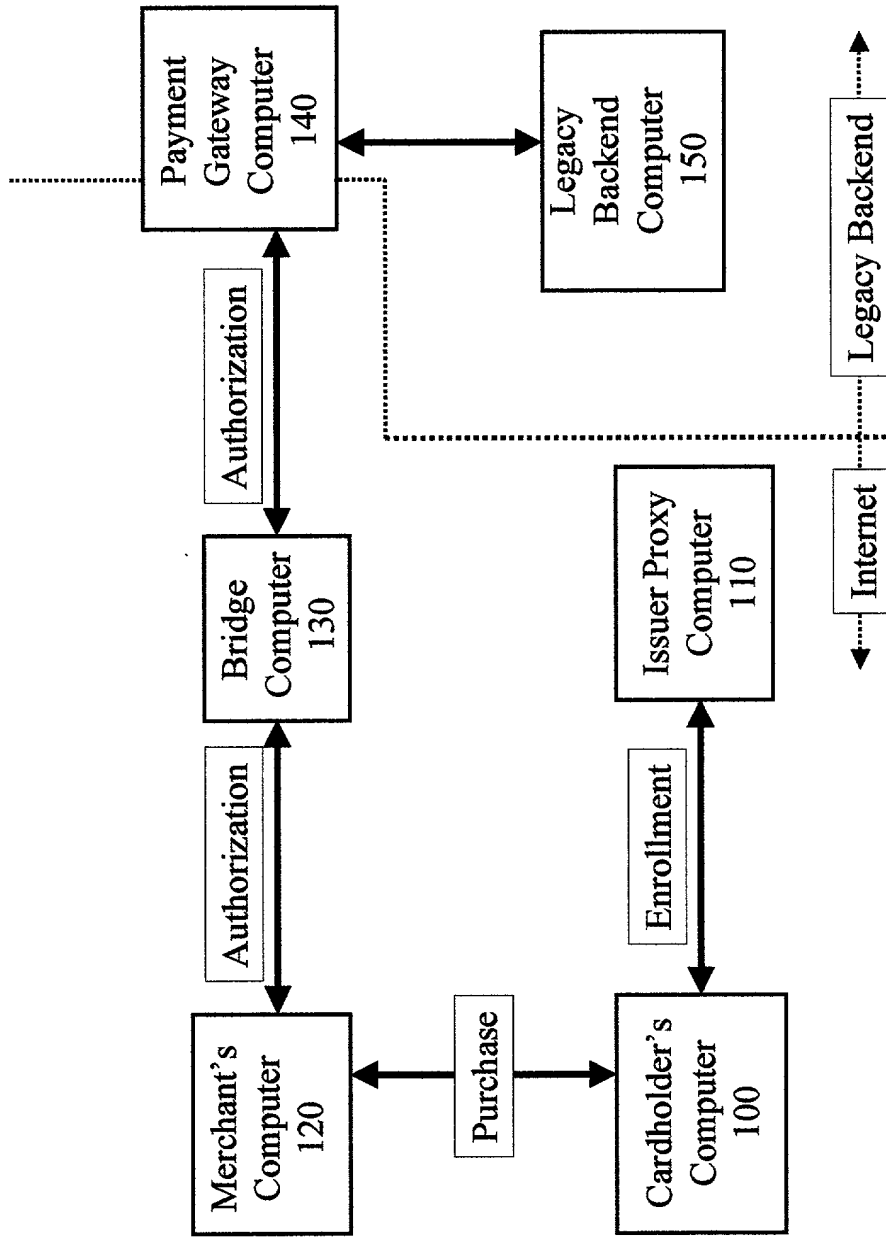


FIG. 1

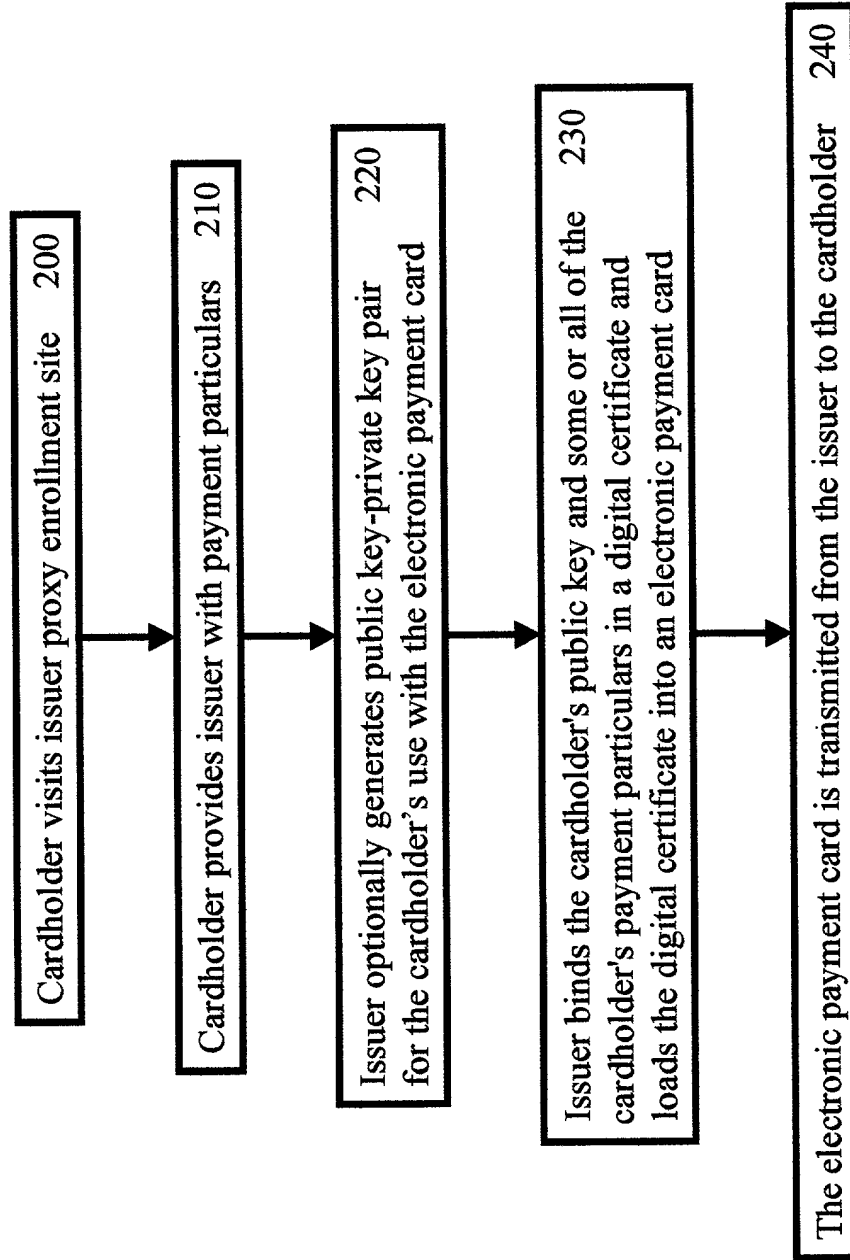


FIG. 2

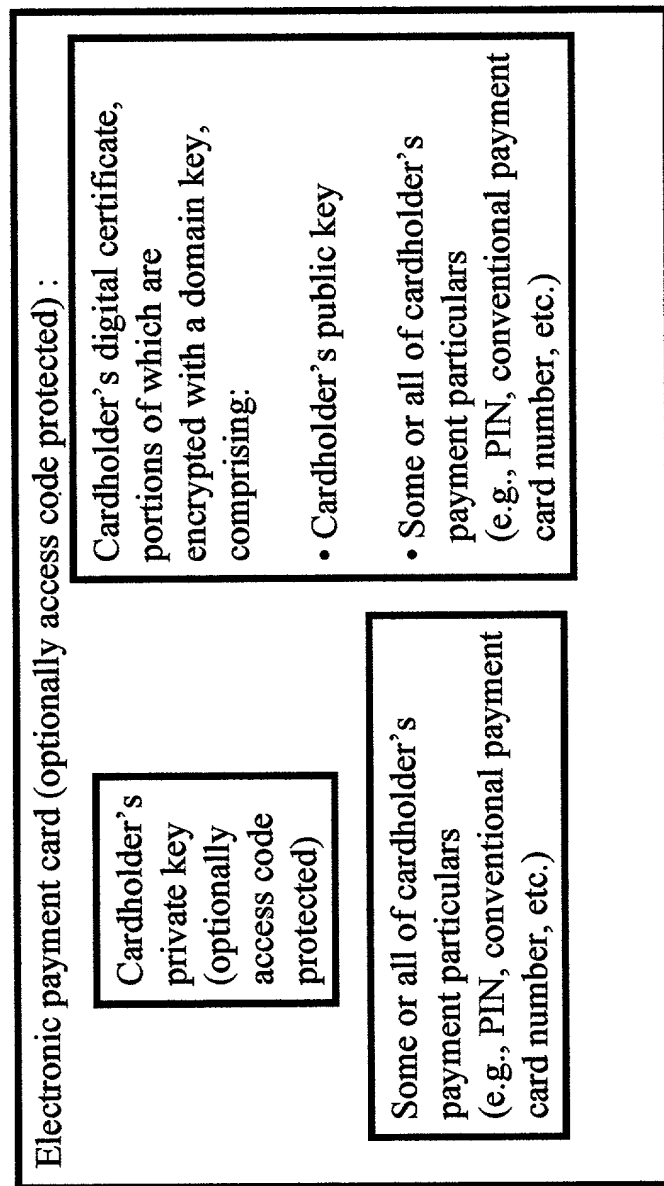


FIG. 2A

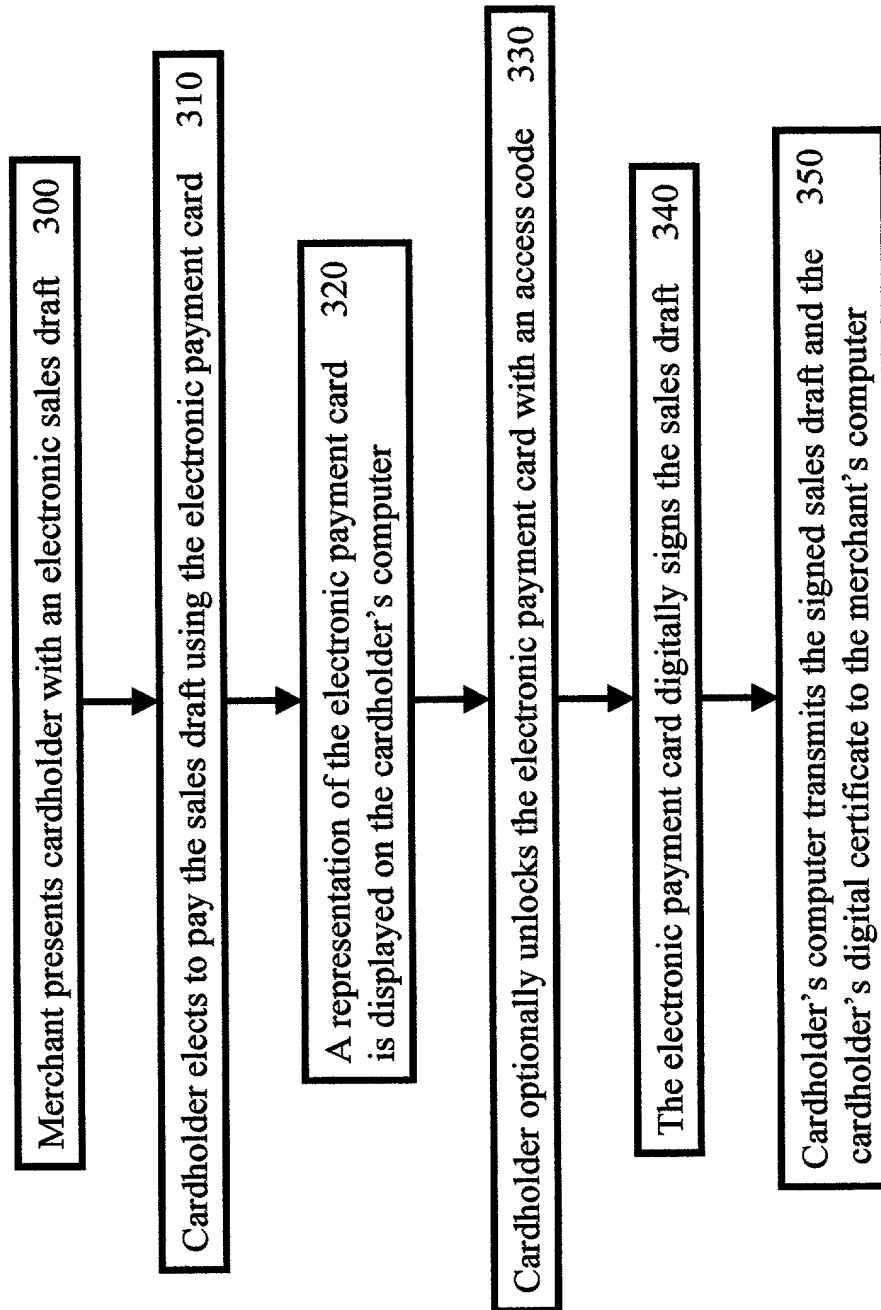


FIG. 3

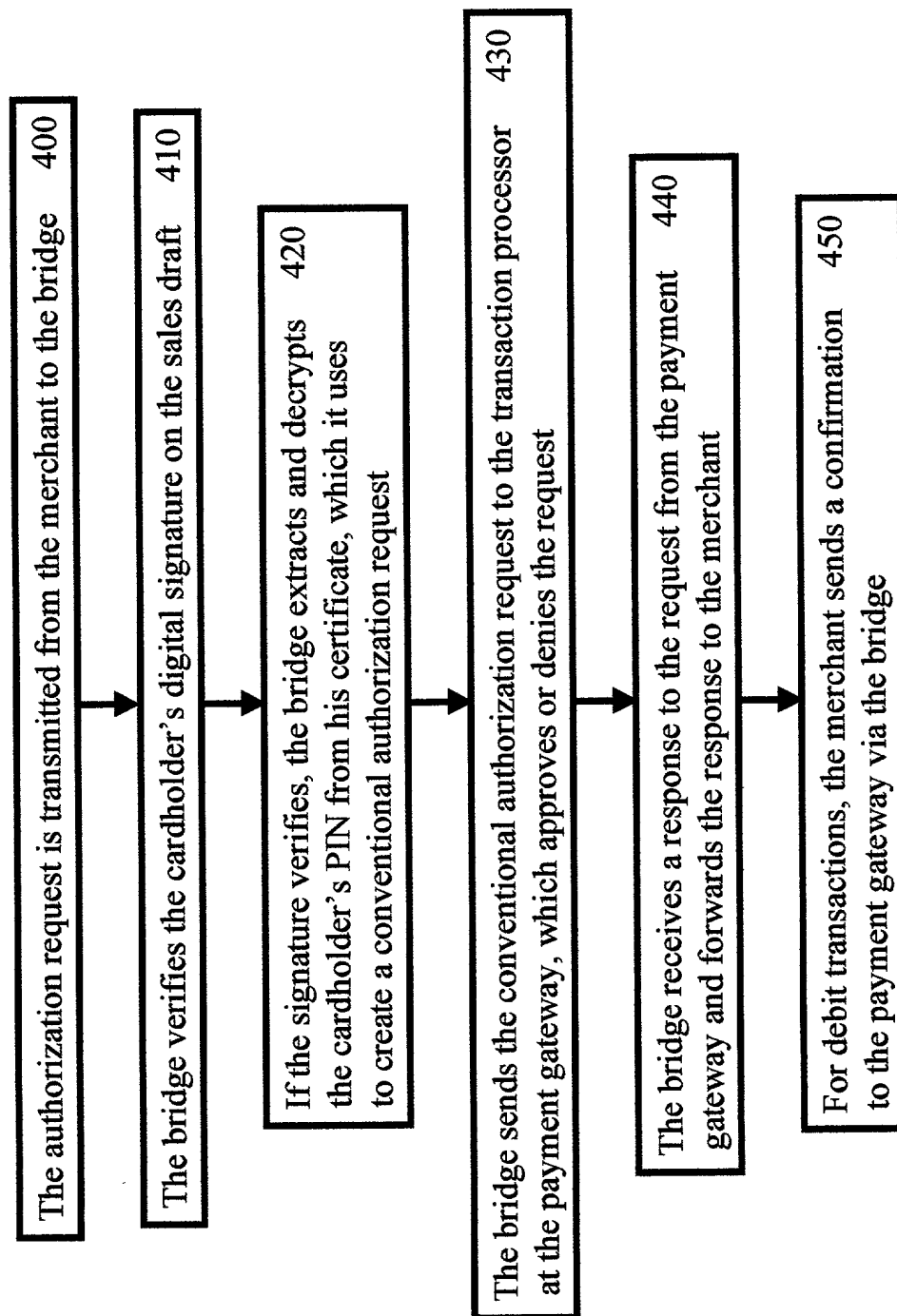


FIG. 4

## DECLARATION FOR PATENT APPLICATION

As below named inventor, I hereby declare that:

My residence and citizenship is as stated below next to my name.

I believe I am the original inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled "**Method and System for Secure Authenticated Payment on a Computer Network**" the specification of which

  X   is attached hereto.

       was filed on                      as  
Application Serial Number                       
and as amended on [date].

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56 (a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate, listed below and so identified, and I have also identified below any foreign application for patent or inventor's certificate on this invention filed by me or my legal representatives or assigns and having a filing date before that of the application on which priority is claimed.

Number	Country	Day/Month/ Year Filed	Priority Claimed - Yes or No
N/A			

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.



Application Serial No.	Filing Date	Status
N/A		

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of First

Joint Inventor

Balas N. Kausik, Ph.D.

Inventor's signature:

Date: \_\_\_\_\_

Residence:

18079 Reed Knoll Road  
Los Gatos, California 95030  
United States of America

Citizenship:

United States

**In The United States Patent and Trademark Office**

In re Application of:

Assignee: Arcot Systems, Inc.

Inventor(s): Balas Natarajan Kausik, Ph.D.

Serial No.: Unknown

Filed: Herewith

For: Method and System For Secure Authenticated Payment On A Computer Network

CERTIFICATE OF MAILING  
BY "EXPRESS MAIL" UNDER 37 CFR § 1.10

"Express Mail" Mailing Label Number

Date of Deposit: \_\_\_\_\_

I hereby certify that this paper and all enclosures are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" under 37 CFR § 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C., 20231.

Type or Print Name of Person Mailing: Paulette D. Isler

\_\_\_\_\_  
Signature of Person Mailing

**POWER OF ATTORNEY BY ASSIGNEE OF PATENT APPLICATION**

Assistant Commissioner for Patents  
BOX PATENT APPLICATION  
Washington, D.C. 20231

Sir:

As the Assignee of the above-identified patent application, the undersigned hereby appoints the following attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith and request that all correspondence and telephone calls in response to this application be directed to SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP, 525 University Avenue, Palo Alto, California 94301, Telephone No. (650) 470-4500:

Attorney	Registration No.
Ronald S. Laurie	25,431
Joseph Yang	41,387
Thomas Raleigh Lane	42,781

Pursuant to 37 C.F.R. § 3.73(b), the undersigned certifies that it is the owner and Assignee of the entire right, title and interest in the above-identified patent application by virtue of assignment from the inventors to the Assignee.

Ownership by the Assignee is established as follows:

- An assignment from the inventors of the matter identified above was recorded at the United States patent and Trademark Office on [ ] at Reel [ ], Frame(s) [ ] through [ ].
- X An assignment from the inventors of the matter identified above is being filed herewith.

The undersigned has reviewed all the documents in the chain of title of the patent application matter identified above, and to the best of his knowledge and belief, title is in the Assignee identified above.

The undersigned hereby declares that all statements made herein of his own knowledge are true, and that all statements made on information and belief are believed to be true; and further, that these statements are made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under § 1001, title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Date: \_\_\_\_\_

Respectfully submitted,  
ARCOT SYSTEMS, INC.

By: \_\_\_\_\_  
Balas Natarajan Kausik, Ph.D.  
President and Chief Executive Officer